Claims

1. A method for facilitating secure data communications using a secret key for encrypting data flowing between first and second entities over a communications link, the method comprising: determining that the communications link has been idle; determining that there is data to flow over the previously idle communications link; and responsive to determining that there is data to flow over the previously idle communications link, initiating generation of a new secret key, the new secret key for encrypting data sent between the first and the second entities over the communications link.

2. The method of claim 1 comprising: determining when a preconfigured amount of data has been sent over the communications link; and responsive to determining that a preconfigured amount of data has been sent over the communications link, initiating generation of a new secret key.

3. The method of claim 1 or 2, wherein the step of determining that the communications link has been idle comprises: determining that the communications link has been idle for at least a predetermined amount of time.

4. The method of claim 3, wherein the step of responsive to determining that there is data to flow over the previously idle communications link, initiating generation of a new secret key comprises: responsive to determining that the link has been idle for at least the predetermined amount of time, initiating generation of a new secret key.

5. The method of claim 3 comprising: responsive to determining that the communications link has been idle for a predetermined period of time, informing the second entity via a heartbeat that the first entity is still present.

6. The method of claim 5 comprising: receiving a reply from the second entity confirming receipt of a heartbeat from the first entity.

7. The method of claim 5 or 6 comprising: responsive to not having received confirmation of receipt of a heartbeat within a predetermined amount of time, terminating communication by the first entity with the second entity.

8. The method of claim 5 or 6 comprising: responsive to not having received confirmation of receipt of a heartbeat within a predetermined period of time, initiating generation of a new secret key before permitting data to be transmitted by the first entity to the second entity.

9. The method of any of claims 5 to 7, wherein the step of determining that the communications link has been idle comprises: determining that the link has been idle enough to cause the first entity to send a heartbeat to the second entity.

10. The method of claim 9, wherein the step of responsive to determining that there is data to flow over the previously idle communications link, initiating generation of a new secret key comprises: responsive to determining that the link has been idle enough to cause the first entity to send a heartbeat to the second entity, initiating generation of a new secret key.

11. The method of any preceding claim, comprising: initiating authentication of at least the second entity prior to initiation of the generation of a new secret key.

12. The method of any preceding claim wherein generation of a new secret key is as a result of a negotiation process carried out between the first and the second entity.

13. A method for facilitating secure data communications using a secret key for encrypting data flowing between the first and the second entities over a communications link, the method comprising: determining that the communications link has been idle; and responsive to determining that the communications link has been idle, ignoring data encrypted with the secret key.

14. The method of claim 13 comprising: accepting only subsequent data encrypted with a newly generated secret key.

15. The method of claim 13 or 14, wherein the step of determining that the communications link has been idle comprises: determining that the communications link has been idle for at least a predetermined amount of time.

16. The method of claim 15, wherein the step of determining that the communications link has been idle for at least a predetermined amount of time comprises: determining that the communications link has been idle for at least a predetermined amount of time via the receipt of a heartbeat from the first entity.

17. The method of claim 15 or 16 comprising: responsive to determining that the communications link has been idle for at least a predetermined amount of time and that no heartbeat has been received from the first entity, terminating communication with the first entity.

18. The method of claim 15 or 16 comprising: responsive to determining that the communications link has been idle for at least a predetermined amount of time

and that no heartbeat has been received from the first entity, accepting only subsequent data encrypted with a newly generated secret key.

19. An apparatus for facilitating secure data communications using a secret key for encrypting data flowing between first and second entities over a communications link, the apparatus comprising: means for determining that the communications link has been idle; means for determining that there is data to flow over the previously idle communications link; and means, responsive to determining that there is data to flow over the previously idle communications link, for initiating generation of a new secret key, the new secret key for encrypting data sent between the first and the second entities over the communications link.

20. The apparatus of claim 19 comprising: means for determining when a preconfigured amount of data has been sent over the communications link; and means for responsive to determining that a preconfigured amount of data has been sent over the communications link, initiating generation of a new secret key.

21. The apparatus of claim 19 or 20, wherein the means for determining that the communications link has been idle comprises: means for determining that the communications link has been idle for at least a predetermined amount of time.

22. The method of claim 21, wherein the means, responsive to determining that there is data to flow over the previously idle communications link, for initiating generation of a new secret key comprises: means, responsive to determining that the link has been idle for at least the predetermined amount of time, for initiating generation of a new secret key.

23. The apparatus of claim 21 comprising: means, responsive to determining that the communications link has been idle for a predetermined period of time, for informing the second entity via a heartbeat that the first entity is still present.

24. The apparatus of claim 23 comprising: means for receiving a reply from the second entity confirming receipt of a heartbeat from the first entity.

25. The apparatus of claim 23 or 24 comprising: means, responsive to not having received confirmation of receipt of a heartbeat within a predetermined amount of time, for terminating communication by the first entity with the second entity.

26. The apparatus of claim 23 or 24 comprising: means, responsive to not having received confirmation of receipt of a heartbeat within a predetermined period of time, for initiating generation of a new secret key before permitting data to be transmitted by the first entity to the second entity.

27. The apparatus of any of claims 23 to 25, wherein the means for determining that the communications link has been idle comprises: means for determining that the link has been idle enough to cause the first entity to send a heartbeat to the second entity.

28. The apparatus of claim 27, wherein the means, responsive to determining that there is data to flow over the previously idle communications link, for initiating generation of a new secret key comprises: means, responsive to determining that the link has been idle enough to cause the first entity to send a heartbeat to the second entity, for initiating generation of a new secret key.

29. The apparatus of any of claims 19 to 29, comprises: means for initiating authentication of at least the second entity prior to initiation of the generation of a new secret key.

30. The apparatus of any of claims 19 to 29 wherein generation of a new secret key is as a result of a negotiation process carried out between the first and the second entity.

31. An apparatus for facilitating secure data communications using a secret key for encrypting data flowing between a first and a second entity over a communications link, the apparatus comprising: means for determining that the communications link has been idle; and means, responsive to determining that the communications link has been idle, for ignoring data encrypted with the secret key.

32. The apparatus of claim 31 comprising: means for accepting only subsequent data encrypted with a newly generated secret key.

33. The method of claim 31 or 32, wherein the means for determining that the communications link has been idle comprises: means for determining that the communications link has been idle for at least a predetermined amount of time.

34. The apparatus of claim 33, wherein the means for determining that the communications link has been idle for at least a predetermined amount of time comprises: means for determining that the communications link has been idle for at least a predetermined amount of time via the receipt of a heartbeat from the first entity.

35. The apparatus of claim 33 or 34 comprising: means, responsive to determining that the communications link has been idle for at least a predetermined amount

of time and that no heartbeat has been received from the first entity, for terminating communication with the first entity.

36. The apparatus of claim 33 or 34 comprising: means, responsive to determining that the communications link has been idle for at least a predetermined amount of time and that no heartbeat has been received from the first entity, for accepting only subsequent data encrypted with a newly generated secret key.

37. A computer program comprising program code means adapted to perform the method of any of claims 1 to 18 when said program is run on a computer.

38. A computer program product comprising computer program code stored on a computer readable storage medium, the program code adapted to perform the method of any of claims 1 to 18 when said program code is run on a computer.